COMMONWEALTH of VIRGINIA

Department of Information Technology

110 SOUTH SEVENTH STREET

RICHMOND, VIRGINIA 23219

(804) 371-5000

Network Security Advisory

To: MIS Directors
Security Officers

From: Don Kendrick,
Chief Security Architect

Re: Microsoft IIS 5.0 Buffer Overflow Update

Date: 24 April 2003

On March 17, 2003, DIT received notification from TruSecure, Microsoft and CERT concerning a serious threat - a buffer overflow that exists in Microsoft IIS 5.0 running on Microsoft Windows 2000. At that time DIT distributed an e-mail advisory to all agencies. The level of the alert was rated RED HOT by TruSecure, the highest risk on a 6 point scale. This is an update to that advisory.

According to the previous alert (refer to http://www.cert.org/advisories/CA-2003-09.html), any attacker who can reach a vulnerable web server can gain complete control of the system and execute arbitrary code in the Local System security context.

DIT has learned that the vulnerabilities described in our earlier alert apply to Windows NT 4.0 version of NTDLL.DLL and therefore the alert has been expanded to include all Windows NT 4.0 systems. NTDLL.DLL is universal on Windows NT and Win2K systems, and is a core part of the Operating Systems.

It is recommended that you apply patch immediately to all affected systems, addressing critical systems first. The patch is available at http://www.microsoft.com/technet/security/bulletin/MS03-007.asp.